**UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF MICHIGAN**
**SOUTHERN DIVISION (DETROIT)**

***In re StockX Customer Data Security Breach Litigation***

Case No.: 2:19-CV-12441-VAR-EAS

Hon. Victoria A. Roberts
Mag. Elizabeth A. Stafford

**FIRST AMENDED CLASS ACTION COMPLAINT**

1. **Violations of Cal. Civ. Code § 1798.81.5;**
2. **Declaratory Judgment; and**
3. **Violations of California Business and Professions Code §§ 17200, *et seq.***

**JURY TRIAL DEMANDED**

Plaintiff Laura Esquer ("Plaintiff"), by and through her counsel, brings this Class Action Complaint against StockX, LLC ("StockX" or "Defendant") on behalf of herself, all others similarly situated, and other members of the general public of the State of California, and alleges upon personal knowledge as to her own actions, and upon information and belief as to counsel's investigations and all other matters, as follows:

## NATURE OF THE ACTION

1. Plaintiff brings this consumer class action against StockX, a Detroit-based company primarily known for its e-commerce platform, StockX.com. Plaintiff seeks a public injunction after StockX failed to secure and safeguard its customers' private information, including the names, shipping addresses, email addresses, and passwords ("Customer Data") of those who created accounts on the StockX website.

2. In August of 2019, several media outlets reported that a hacker had stolen more than 6.8 million customer records from Defendant's website in May of 2019 (the "Data Breach").[1]

3. Despite knowing its records had been hacked, Defendant failed to inform its users and instead tried to hide the fact by sending out a notification telling

[1] *See*, *e.g.,* Zach Whittaker, *StockX was hacked, exposing millions of customers' data*, TechCrunch (Aug. 3, 2019, 12:00 PM) *available at* https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/. (last visited July 7, 2021).

its users to reset their passwords, under the guise of "system updates."[2]

4. However, a prominent technology publication was contacted by the stolen data's seller, who claimed that more than 6.8 million records were stolen from Defendant.[3]

5. The seller informed the prominent technology publication that the seller had already placed the data for sale, and, in fact, had already sold the data to criminals on the dark web.[4] The technology publication subsequently contacted a sample of consumers who had their data stolen, with each consumer "confirm[ing] their data as accurate."[5]

6. Had StockX detected the Data Breach earlier, less data would have been stolen and customers would have been able to take earlier action to mitigate their damages.

7. For these reasons, StockX disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable data-security measures to ensure its systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to monitor and detect the breach on a timely basis, and failing to disclose to its

---

2 *Id.*
3 *Id.*
4 *Id.*
5 *Id.*

customers the material facts that it did not have adequate security systems and practices to safeguard Customer Data.

8. The private Customer Data obtained from the data breach was compromised due to StockX's acts and omissions and its failure to properly protect the Customer Data. If StockX had maintained and implemented proper data-security measures to safeguard Customer Data, deter the criminal hackers that orchestrated the Data Breach, and detect the breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented, or at the very least, its harm mitigated.

9. StockX knew, or should have known, that its data security measures were inadequate. StockX's Data Breach followed prominent breaches involving other e-commerce websites such as shein.com, panerabread.com, adidas.com, orbitz.com, macys.com, bloomingsdales.com, and zappos.com.

10. As a result of the Data Breach, Plaintiff's and Class members' Customer Data has been exposed to criminals for misuse. The injuries suffered or that will likely be suffered by Plaintiffs and Class members as a direct result of StockX's data breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection, prevention, and mitigation of the unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the data breach including but not limited to foregoing cash back rewards;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the StockX data breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Customer Data being placed in the hands of criminals and already misused via the use of Plaintiff's and Class members' Customer data on the Internet black market, including in illegal "credential stuffing" schemes. This is especially important because StockX did not warn Plaintiff and other Class members of the impact of credential stuffing on their other e-commerce accounts;

h. damages to and diminution in value of their Customer Data entrusted to StockX for the sole purpose of using the StockX website, and with the mutual understanding that StockX would safeguard Plaintiff's and Class members' data against theft and not allow access to and misuse of their information by others; and

i. the continued risk to their Customer Data which remains in the possession of StockX and which is subject to further breaches so long as StockX fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

11. These injuries to Plaintiff and Class members were directly and proximately caused by StockX's failure to implement or maintain adequate data security measures for Customer Data.

12. Plaintiff, Class members, and members of the public have a significant interest in ensuring that their Customer Data and any other customer data others may provide StockX, is protected from future breaches.

13. Plaintiff, on behalf of herself and similarly situated consumers, seeks equitable relief in the form of public injunctive relief to prevent a reoccurrence of the data breach and resulting injury, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

## JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy, based on the injunctive relief sought in this case, exceeds $5 million exclusive of interest and costs, there are more than 100 putative class members, and all the putative class member and StockX are citizens of different states.

15. This Court has personal jurisdiction over StockX because StockX has sufficient minimum contacts in California and intentionally avails itself of this jurisdiction by marketing, distributing, and selling products throughout California, including this District.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims occurred in this

District. Specifically, Plaintiff created her StockX account by providing her Customer Data to StockX in this District.

## PARTIES

### A. Plaintiff

17. Plaintiff is a citizen of the state of California and a resident of San Jose, California. In early to mid-2019, Plaintiff created an account with StockX, providing her email address and creating a password for login.

18. In or around early August 2019, Plaintiff received an email alert from Defendant, recommending that she reset her password for the StockX website. However, in that email, Defendant did not disclose that there had been a data breach, and instead requested that she reset her password because of "system updates." This statement was false and deceptive as, at the time, Defendant had known that its customers' data had actually been hacked.

19. Plaintiff's Customer Data was stolen in the Data Breach. Plaintiff has received two notifications on her CreditWise credit report confirming that the email address and password she used to create her StockX account was compromised as a result of StockX's data breach.

20. As a result of the data breach, Plaintiff has expended 10 minutes reading and reviewing her credit report. Furthermore, Plaintiff has expended 20 minutes trying to figure out how to change her password on the StockX website.

21. Plaintiff would not have created a StockX account had StockX told her that it lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft.

22. Plaintiff suffered actual injury from having her Customer Data compromised and stolen as a result of the StockX data breach.

23. Plaintiff and Class members suffered actual injury in the form of damages to and diminution in the value of their Customer Data – a form of intangible property that they entrusted to StockX for the purpose of using StockX and that was compromised in and as a result of StockX's Data Breach. Because Plaintiff's and Class members' Customer Data remain in the hands of criminals, a criminal marketplace exists for the data (as is confirmed by the fact that the stolen information has already been sold) and they have lost the sales value of this data. Therefore, Plaintiff and Class members have suffered from the diminution of value of their Customer Data.

24. Plaintiff and Class Members have suffered and will continue to suffer imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their Customer Data being placed in the hands of criminals who have already misused such information stolen in the Data Breach via sale of the Customer Data on the internet black market. This future threat is particularly materialized given the prevalence of "credential stuffing," a method

used by hackers to gain additional, private information from a victim via stolen login credentials (explained in greater detail in Paragraphs 32, 43-44, and 59). Therefore, Plaintiff and Class members have a continuing interest in ensuring that their private information, which remains in StockX's possession, is protected and safeguarded from future breaches.

25. Plaintiff wishes to and is likely to continue using the StockX website if StockX's data security and policies was improved to protect against future data breaches. However, absent an injunction, Plaintiff cannot be certain whether the StockX website is safe to use or not.

**B. Defendant**

26. Defendant StockX, Inc. is a Michigan limited liability company with its principal place of business located at 1046 Woodward Avenue, Detroit, Michigan 48226. StockX operates an online marketplace via its website, www.StockX.com. StockX is an e-commerce platform on which consumers throughout California, including in this District, can buy and sell like-new merchandise including, but not limited to sneakers, watches, handbags and street wear.

## STATEMENT OF FACTS

**A. Value of Customer Data On the Cyber Black Market**

27. Stolen private information is a valuable commodity. A "cyber black-market", exists in which criminals openly post stolen payment card numbers, social

security numbers, and other personal information on a number of underground Internet websites. The private data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

28. Legitimate organizations and the criminal underground alike recognize the value in private personal data contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it.

29. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[7]

30. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "[t]hey might steal your name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers" as well as "buy things with your credit cards," "buy

[6] 17 C.F.R § 248.201 (2013).
[7] *Id*.

things with your credit cards," and "open a phone, electricity, or gas" in the victim's name.[8]

31. Identity thieves can use personal information, such as that of Plaintiff and Class members which StockX failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

32. Highly relevant to this particular Data Breach, hackers can engage in "credential stuffing," a type of cyberattack where stolen account login credentials are used to gain unauthorized access to a user's other online accounts through large-scale automated login requests directed against a web application.[9] This is "a bit like a thief finding a ring of keys in an apartment lobby and trying them, one after the other, in every door in the building. Software makes the trial-and-error process practically instantaneous."[10] This very often result in a "ripple effect" where the

[8] Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 7, 2021).

[9] https://www.owasp.org/index.php/Credential_stuffing (last visited July 7, 2021).

[10] https://www.neweurope.eu/article/password-breach-ripple-effects-well-beyond-yahoo/ (last visited July 7, 2021).

hackers gain unauthorized access to other personal data stored on a consumer's other online accounts, such as payment card data, social security numbers, driver license numbers, addresses, and even other account credentials.

33. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[11]

34. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[12]

35. There may be a time lag between when harm occurs versus when it is discovered, and also between when customer data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity

[11] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited July 7, 2021).

[12] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 7, 2021).

theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

## B. StockX Had Notice of Data Breaches Involving E-Commerce Websites

36. At all relevant times, StockX knew, or reasonably should have known, of the importance of safeguarding the highly sensitive Customer Data and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

37. In 2018, the number of U.S. data breaches was approximately 1,244. The 2019 number has surpassed this with over 3,800 publicly disclosed breaches.[14]

38. More specifically, a significant number of the data breaches in the past few years have targeted other e-commerce websites like StockX, including data

[13] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at* https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited July 7, 2021).

[14] Rebecca Nanako Juchems, *Enough is Enough: 2018 Has Seen 600 Too Many Data Breaches*, (July 24, 2018) *available at* https://medium.com/@AxelUnlimited/enough-is-enough-2018-has-seen-600-too-many-data-breaches-9e3e5cd8ff78 (last visited July 7, 2021).

breaches affecting shein.com, panerabread.com, adidas.com, orbitz.com, macys.com, bloomingsdales.com, and zappos.com.

39. Unfortunately, and as alleged below, despite all the publicly available knowledge of the continued compromises of customer data, especially in the e-commerce industry, StockX's approach to maintaining the privacy and security of the Plaintiff's and Class members' Consumer Data was lackadaisical, cavalier, reckless, or at the very least, negligent.

## C. StockX Failed to Comply With FTC Requirements

40. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental

[15] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 7, 2021).

data security principles and practices for business.[16] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC also recommends that companies limit access to sensitive data, require complex and secure passwords to be used on networks, require authentication, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[17]

---

[16] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited July 7, 2021).

[17] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 7, 2021).

43. Specifically, the FTC has observed that "[c]onsumers and employees often reuse usernames and passwords across different online accounts, making those credentials extremely valuable to remote attackers."[18] As a result, "[c]redentials are sold on the dark web and used to perpetrate credential stuffing attacks – a kind of attack in which hackers automatically, and on a large scale, input stolen usernames and passwords into popular internet sites to determine if any of them work."[19]

44. To combat credential stuffing, the FTC requires companies to "combine multiple authentication techniques," such as strong password requirements, two-factor authentication, and credential screening.[20] [21]

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from

[18] https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication (last visited July 7, 2021).
[19] *Id*.
[20] https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-require-secure-passwords-authentication (last visited July 7, 2021).
[21] https://www.passwordping.com/ftc_credential_stuffing_ato/ (last visited July 7, 2021).

these actions further clarify the measures businesses must take to meet their data security obligations.

46. StockX's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including by requiring more complex and unique passwords, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. StockX's failure to warn affected consumers about the substantial risk of credential stuffing also constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. In this case, StockX was at all times fully aware of its obligation to protect the private data of its customers. StockX was also aware of the significant repercussions if it failed to do so because StockX collects private information from millions of customers and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

48. Despite understanding the consequences of inadequate data security, StockX failed to comply with FTC requirements and failed to take additional protective measures beyond those required by FTC.

## D. The StockX Data Breach

49. On July 26, 2019, StockX discovered that its customers' Customer Data was stolen in a cyberattack, resulting in the unauthorized access of at least 6.8

million users' records.[22]

50. The Data Breach was active from approximately May 2019 to late July 2019.[23]

51. On August 1, 2019, StockX emailed users instructing them to change their passwords in connection with "system updates."[24]

52. On August 3, 2019, TechCrunch reported being contacted by an unnamed data breach seller claiming over 6.8 million StockX user records had been stolen in May 2019 by a hacker. The unnamed seller claimed to have sold the stolen data on the dark web.[25]

53. Following TechCrunch's August 3 report, StockX disclosed the hack publicly, acknowledging that it only prompted users to reset their customer

---

[22] StockX, *Notice of Data Breach*, (Aug. 8, 2019) available at *https://s3.amazonaws.com/stockx-sneaker-analysis/wp-content/uploads/2019/08/StockX-Notice-of-Data-Breach-8.8.19.pdf*; Zach Whittaker, *StockX was hacked, exposing millions of customers' data*, TechCrunch (Aug. 3, 2019, 12:00 PM) *available at* https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/ (last visited July 7, 2021).

[23] StockX, *Notice of Data Breach*, (Aug. 8, 2019).

[24] Zach Whittaker, *StockX admits 'suspicious activity' led to resetting passwords without warning*, TechCrunch (Aug. 1, 2019, 7:05 PM) *available at* https://techcrunch.com/2019/08/01/stockx-security-concerns-reset-passwords/ (last visited July 7, 2021).

[25] Zach Whittaker, *StockX was hacked, exposing millions of customers' data*, TechCrunch (Aug. 3, 2019, 12:00 PM) *available at* https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/. (last visited July 7, 2021).

passwords after it was "alerted to suspicious activity" on its site, despite telling users it was a result of "system updates."[26]

54. The stolen Customer Data included customer names, email addresses, user passwords and other profile information.

55. Additionally, StockX attempted to mask the breach by emailing its customers instructions to reset their passwords in connection with "system updates."

56. Had StockX implemented and maintained adequate safeguards to protect the Customer Data, deter the hackers, and detect the data breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented and customers would have been able to take earlier action to mitigate their damages.

57. In permitting the Data Breach to occur, StockX breached its implied agreement with customers to protect their personal and financial information and violated industry standards.

## E. The StockX Data Breach Has Caused Harm and Will Result In Future Harm

58. Plaintiff's and Class members' Consumer Data is private and sensitive in nature and was left inadequately protected by StockX. StockX did not obtain

[26] Zach Whittaker, *StockX admits 'suspicious activity' led to resetting passwords without warning*, TechCrunch (Aug. 1, 2019, 7:05 PM) *available at* https://techcrunch.com/2019/08/01/stockx-security-concerns-reset-passwords/ (last visited July 7, 2021).

Plaintiff's and Class members' consent to disclose their Customer Data to any unauthorized persons as required by applicable law and industry standards.

59. With the known Customer Data stolen, criminals can engage in "credential stuffing," a type of cyberattack where stolen account credentials (typically usernames, emails, and passwords) are used to gain unauthorized access to a user's other accounts through large-scale automated login requests directed against a web application.[27] It is estimated that credential stuffing bots access 3-8% of the target accounts using compromised credentials from the dark web.[28] As a result of the "ripple effect" of credential stuffing, hackers can obtain a consumer's other personal and sensitive information, including payment card information, social security numbers, driver license numbers, addresses, and other login credentials.

60. The StockX Data Breach was a direct and proximate result of its failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including StockX's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class

[27] Neal Mueller, *Credential stuffing*, OWASP, https://www.owasp.org/index.php/Credential_stuffing (last visited July 7, 2021).
[28] https://www.passwordping.com/ftc_credential_stuffing_ato/ (last visited July 7, 2021).

members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

61. Due to StockX's failure to adequately secure the Customer Data and timely identify the breach, the hackers were able to extract sensitive personal data from StockX's customers for approximately two months. Customers, including Plaintiff and Class members, have been left exposed, unknowingly and unwittingly, to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

62. As a direct and proximate result of StockX's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to expend money and take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, updating credentials, and filing police reports. This time has been lost forever and cannot be recaptured.

63. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

64. As a result of the Data Breach, Plaintiff's and Class members' Customer Data has been exposed to criminals for misuse. The injuries suffered or that will likely be suffered by Plaintiff and Class members as a direct result of StockX's data breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection, prevention, and mitigation of the unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the data breach including but not limited to foregoing cash back rewards;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the StockX data breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Customer Data being placed in the hands of criminals and already misused via the use of Plaintiff's and Class members' Customer data on the Internet black market, including in illegal "credential stuffing" schemes. This is especially important because StockX did not warn Plaintiff and other Class members of the impact of credential stuffing;

h. damages to and diminution in value of their Customer Data entrusted to StockX for the sole purpose of purchasing products StockX and with the mutual understanding that StockX would safeguard Plaintiff's and Class members' data against theft and not allow access to and misuse of their information by others; and

i. continued risk to their Customer Data which remains in the possession of StockX and which is subject to further breaches so long as StockX fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data in its possession.

65. While the Plaintiff's and Class members' Consumer Data has been stolen, StockX continues to hold Customer Data of its customers. Particularly because StockX has demonstrated an inability to prevent a breach or detect it after running unhindered for approximately two months, Plaintiff and members of the Class have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

## CLASS ALLEGATIONS

66. Plaintiff seeks relief on behalf of herself and as the representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), Plaintiff seeks to certify a class of all citizens of California whose Customer Data was stolen from StockX during the Data Breach (the "Class").

67. Excluded from each of the Class is StockX and any of its parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judges to whom this case is assigned as well as his or her judicial staff and immediate family members.

68. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

69. Plaintiff is a member of the Class.

70. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a) and (b)(2):

71. **Numerosity.** The proposed Class includes at least hundreds of thousands of customers whose data was compromised in the breach. The massive size of the StockX data breach indicates that joinder of each member would be impracticable.

72. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. Whether StockX had a duty to protect the Customer Data;

b. Whether StockX knew or should have known of the susceptibility of their data security to a data breach;

c. Whether StockX's security measures to protect their data were reasonable in light of the FTC data security requirements, and other measures recommended by data security experts;

d. Whether StockX was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether StockX's failure to implement adequate data security measures allowed the data breach;

f. Whether StockX's conduct constituted unfair, unlawful, and/or deceptive trade practices under California law;

g. Whether StockX's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Customer Data of Plaintiff and Class members;

h. Whether StockX was negligent as a result of its possible violation of relevant statutes, such as Cal. Civ. Code Sections 1798.81.5;

i. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief.

73. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of the claims of the Class. Plaintiff and Class members were injured through StockX's uniform misconduct and their legal claims arise from the same core practices employed or omitted by StockX.

74. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiff is an adequate representative of the proposed Class because her interests do not conflict with the

interests of the Class members she seeks to represent. Plaintiff's counsel are experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive retail data breach cases.

75. **Superiority. Fed. R. Civ. P. 23(a)(5).** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against StockX. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

76. **Injunctive and Declaratory Relief.** Class certification is appropriate under Fed. R. Civ. P. 23(b)(2). StockX has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

77. Finally, all members of the proposed Class are readily ascertainable. StockX has access to information regarding which customers' Customer Data was affected by the breach, the time period of the breach, as well as the addresses and

other contact information for members of the Class, which can be used for providing notice to the Class members.

**COUNT I**
**Violation Of Cal. Civ. Code § 1798.81.5**
**(*On Behalf Of The Class*)**

78. Plaintiff restates and realleges paragraphs 1 through 77 above as if fully set forth herein.

79. Cal Civ. Code § 1798.81.5(a)(1) provides that its purpose is to "ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

80. Cal. Civ. Code § 1798.81.5(b) provides, in pertinent part, that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

81. Under Cal Civ. Code § 1798.81.5(d)(1)(B), "personal information" means a "username or email address in combination with a password or security question and answer that would permit access to an online account."

82. Therefore, the Customer Data stolen in the StockX Breach, which

includes Plaintiff and Class members' email addresses and passwords, falls within the meaning of "personal information" under Cal. Civ. Code Section 1798.81.5.

83. By failing to implement adequate and reasonable data security measures for this Customer Data, StockX violated Cal. Civ. Code Section 1798.81.5.

84. Because StockX violated Cal. Civ. Code Sections 1798.81.5, Plaintiff may seek an injunction pursuant to Cal. Civ. Code Section 1798.84(e), which states "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined." Specifically, Plaintiff seeks injunctive relief requiring StockX to implement and maintain adequate and reasonable data security measures and abide by the California Data Breach laws, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on StockX's systems periodically, and ordering StockX to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training its security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of StockX's data security measures are compromised, hackers cannot gain access to other areas of StockX's systems;

f. utilizing more complex and multilayered authentication;

g. requiring consumers use more complex and unique passwords;

h. warning consumers of the substantial risks and effects of credential stuffing, instructing affected consumers to change their credentials on other e-commerce and web platforms they use;

i. deleting, in a reasonable and secure manner, Customer Data not necessary for StockX's provisions of products;

j. conducting regular database scanning and security checks;

k. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and

contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

l. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

**COUNT II**
**Declaratory Judgment**
**(*On Behalf Of The Class*)**

85. Plaintiff restates and realleges Paragraphs 1 through 77 as if fully set forth here.

86. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this Complaint.

87. As previously alleged, Plaintiff and Class members entered into an implied contract that required StockX to provide adequate security for the Customer Data it collected from their creating accounts and purchasing goods from the StockX website. As previously alleged, StockX owes duties of care to Plaintiff and Class members that require it to adequately secure that Customer Data.

88. StockX still possesses Customer Data pertaining to Plaintiff and Class members.

89. Accordingly, StockX has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that StockX's lax approach towards data security has become public, the Customer Data in its possession is more vulnerable than previously.

90. Actual harm has arisen in the wake of the StockX Data Breach regarding StockX's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

91. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. StockX continues to owe a legal duty to secure consumers' Customer Data and to timely and accurately notify consumers of the data breach under California law, common law, and Section 5 of the FTC Act;

b. StockX's existing data security measures do not comply with their legal duties of care; and

c. StockX continues to breach its legal duty by failing to employ reasonable measures to secure consumers' Customer Data.

92. Plaintiff also requests an injunction requiring StockX to comply with its contractual obligations and duties of care and implement and maintain reasonable security measures, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on StockX's systems periodically, and ordering StockX to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement[ing] and maintain[ing] reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training its security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of StockX's data security measures are compromised, hackers cannot gain access to other areas of StockX's systems;

f. utilizing more complex and multilayered authentication;

g. requiring consumers use more complex and unique passwords;

h. warning consumers of the substantial risks and effects of credential stuffing, instructing affected consumers to change their credentials on other e-commerce and web platforms they use;

i. deleting, in a reasonable and secure manner, Customer Data not necessary for StockX's provisions of goods;

j. conducting regular database scanning and security checks;

k. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

l. educating its customers about the threats they face as a result of the loss of their financial and personal information to third

parties, as well as the steps customers must take to protect themselves.

93. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy in the event StockX incurs another data breach. The risk of another such breach is real, immediate, and substantial.

94. The hardship to Plaintiff and other Class members if an injunction is not issued exceeds the hardship to StockX if an injunction is issued. If StockX incurs another data breach, Plaintiff and other customers will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to StockX of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and StockX has a pre-existing legal obligation to employ such measures.

95. Such an injunction would benefit the public by preventing another data breach for StockX, and therefore eliminating the additional injuries that would result to Plaintiff and the millions of customers whose confidential information would be further compromised.

## COUNT III
**Violation Of California's Unfair Competition Law ("UCL"), California Business & Professions Code §§ 17200, *et seq.***
**(*On Behalf Of The Class*)**

96. Plaintiff restates and realleges Paragraphs 1 through 77 above as if fully set forth herein.

97. UCL § 17200 provides, in pertinent part, that "unfair competition shall mean and include unlawful, unfair, or fraudulent business practices [. . .]"

98. Under the UCL, a business act or practice is "unlawful" if the act or practice violates any established state or federal law.

99. StockX's failures to implement and maintain reasonable security measures and to timely and properly notify Plaintiff and Class members of the Data Breach therefore was and continues to be "unlawful" as StockX breached its implied and express warranties and violated the California laws regarding data breaches, including California Civil Code §§ 1798.81.5, as well as the FTC Act.

100. As a result of StockX's unlawful business acts and practices, StockX unlawfully obtained money from Plaintiff and members of the Class.

101. Under the UCL, a business act or practice is "unfair" if the defendant's conduct is substantially injurious to consumers, goes against public policy, and is immoral, unethical, oppressive, and unscrupulous, as the benefits for committing these acts or practices are outweighed by the severity of the harm to the alleged victims.

102. Here, StockX's reckless conduct was and continues to be of no benefit to its customers, as it is both injurious and unlawful to those persons who rely on

StockX's duties and obligations to maintain and implement reasonable data security measures and to monitor for breaches. Having lax data security measures that has resulted in the disclosure of millions of customers' payment card information provides no benefit to consumers. For these reasons, StockX's conduct was and continues to be "unfair" under the UCL.

103. As a result of StockX's unfair business acts and practices, StockX has unfairly and unlawfully obtained money from Plaintiff and members of the Class.

104. Plaintiff requests that this Court enjoin StockX from violating the UCL or violating the UCL in the same way in the future, as discussed in Paragraph 92 *supra*. Otherwise, Plaintiff and members of the Class may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

## REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against StockX as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiff as representative of the Class; and naming Plaintiff's attorneys as Class Counsel to represent the Class;

b) For an order declaring that StockX's conduct violates the statutes and laws referenced herein;

c) For an order finding in favor of Plaintiff, and the Class, on all counts

asserted herein;

d) For injunctive relief as pleaded or as the Court may deem proper;

e) For an order awarding Plaintiff and all Class their reasonable attorneys' fees, expenses and costs of suit, including as provided by statute such as under the Federal Rules of Civil Procedure 23(h); and

f) For any other such relief as the Court deems just and proper.

**DEMAND FOR TRIAL BY JURY**

Plaintiff demands a trial by jury on all issues so triable.

Dated: July 7, 2021

*s/ Benjamin Heikali*
Benjamin Heikali
**FARUQI & FARUQI, LLP**
10866 Wilshire Blvd., Suite 1470
Los Angeles, CA 90024
Tel: 424.256.2884
Fax: 424.256.2885
bheikali@faruqilaw.com
(CA State Bar No. 307466)

Timothy J. Peter
**FARUQI & FARUQI, LLP**
1617 JFK Blvd. #1550
Philadelphia, PA 19103
(215) 277-5770
tpeter@faruqilaw.com
(PA State Bar No. 306965)

Derek T. Howard
**THE DEREK HOWARD LAW FIRM**
838 W. Long Lake Rd., Ste 100

Bloomfield Hills, MI 48302
(248) 237-7300
derek@howardfirmplc.com
(P69625)

*Counsel for Plaintiff*

**CERTIFICATE OF SERVICE**

I hereby certify that on July 7, 2021 I electronically filed the foregoing with the Clerk of the Court using the CM/ECF filing system, which will send electronic notification of such filing to all counsel of record

/s/ *Derek T. Howard*

**THE DEREK HOWARD LAW FIRM**
838 W. Long Lake Rd., Ste 100
Bloomfield Hills, MI 48302
(248) 237-7300
derek@howardfirmplc.com
(P69625)

*Counsel for Plaintiff*